Legal Standards and Authorities

The following is a description of various laws, regulations and other legal requirements potentially applicable to the various matters identified in the Report.

1. Deception of Congress and the American Public
   a. Committing a Fraud Against the United States (18U.S.C. § 371)
   b. Making False Statements to Congress (18 U.S.C. § 1001)
   c. War Powers Resolution (Public Law 93-148)
   d. Misuse of Government Funds (31 U.S.C. § 1301)

2. Improper Detention, Torture, and Other Inhumane Treatment
   a. Anti-Torture Statute (18 U.S.C. §§ 2340-40A)
   b. The War Crimes Act (18 U.S.C. § 2441)
   c. The Geneva Conventions and Hague Convention: International Laws Governing the Treatment of Detainees
   d. United Nations Convention Against Torture, and Cruel, Inhuman and Degrading Treatment: International Laws Governing the Treatment of Detainees
   e. Command Responsibility
   f. Material Witness (18 U.S.C. § 3144)

3. Retaliating against Witnesses and Other Individuals
   a. Obstructing Congress (18 U.S.C. § 1505)
   b. Whistleblower Protection (5 U.S.C. § 2302)
   c. The Lloyd-LaFollette Act (5 U.S.C. § 7211)
   d. Retaliating against Witnesses (18 U.S.C. § 1513)

4. Leaking and other Misuse of Intelligence and other Government Information
   a. Revealing Classified Information in Contravention of Federal Regulations (Executive Order 12958/ Classified Information Nondisclosure Agreement)
   b. Statutory Prohibitions on Leaking Information

5. Laws and Guidelines Prohibiting Conflicts of Interest

6. Laws Governing Electronic Surveillance
   a. Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 et seq.)
   b. National Security Act of 1947 (50 U.S.C. chapter 15)
   c. Communications Act of 1934 (47 U.S.C. § 222)

d. Stored Communications Act of 1986 (18 U.S.C. § 2702)

e. Pen Registers or Trap and Trace Devices (18 U.S.C. § 3121)

1. Deception of Congress and the American Public

a. Committing a Fraud Against the United States (18 U.S.C. § 371)

This statute makes it a crime, punishable by a fine and up to five years in prison, to conspire "to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy." "Defrauding the government" has been defined quite broadly and does not need an underlying criminal offense and alone subjects the offender to prosecution. United States v. Harmas, 974 F.2d 1262, 1266 (11th Cir. 1992).

For nearly 80 years this statute has been used to prosecute government officials and citizens alike who commit a fraud in the most liberal use of the term. The law is clear: the government need not be defrauded of money or property to trigger this statute. It is enough that the government was prevented from being able to exercise its lawful duties and authorities. As the Supreme Court stated, the law applies to those who:

> interfere with or obstruct one of its lawful governmental functions by deceit, craft or trickery, or at least by means that are dishonest. It is not necessary that the Government shall be subjected to property or pecuniary loss by the fraud, but only that its legitimate official action and purpose shall be defeated by misrepresentation, chicanery or the overreaching of those charged with carrying out the governmental intention. United States v. Harmas, 974 F.2d 1262, 1266 (11th Cir. 1992).

Another more recent case repeats that principle of law. The Second Circuit held that "this statute does not restrict its application to documents that are required to be given to Congress, does not require proof that any statements made to effect the object of the conspiracy were made directly to Congress, and does not require that the conspiracy was successful." United States v. Ballistrea, 101 F.3d 827, 831-832 (2nd Cir. 1996), *cited by* Francis T. Mandanici, *Bush's Uranium Lies: The Case for a Special Prosecutor That Could Lead to Impeachment* (June 29, 2005), *available at* http://democracyrising.us/content/view/269/164. One treatise has defined fraud as "a generic term which embraces all the multifarious means which human ingenuity can devise and are resorted to by one individual to gain an advantage over another by false suggestions or by suppression of the truth." CORPUS JURIS SECUNDUM § 2. Francis T. Mandanici, "Bush's Uranium Lies: The Case for a Special Prosecutor That Could Lead to Impeachment," (June 29, 2005).

Lawrence E. Walsh, Independent Counsel in charge of the Iran-Contra investigation pointed out that the deception of Congress statute applies even when the official is involved in official government policy. In his final report, he concluded, "Fraud is criminal even when those who engage in the fraud are Government officials pursuing presidential policy." LAWRENCE E. WALSH, FINAL REPORT OF THE INDEPENDENT COUNSEL FOR IRAN/CONTRA MATTERS, VOLUME I: INVESTIGATIONS AND PROSECUTIONS, Aug. 4, 1993.

Under these precedents, anyone - including the President and his Administration - is prohibited from intentionally misleading the Congress or any other part of the government in pursuit of his or her policy. While this statute is similar to obstructing or lying to Congress (described below), it is broader. It covers acts that may not technically be lying or communications that are not formally before Congress. Indeed, it need only be "overreaching," in the words of the Supreme Court, *(Hammerschmidt*, 265 U.S. at 188.) an exaggeration, if the intent is to influence the government.

This statute was used in the prosecution of numerous Administration and military officials in the Iran-Contra scandal. *Ibid.* It was also used by the Justice Department to prosecute members of the Nixon Administration who used the CIA to interfere with the FBI investigation of the Watergate break-in. United States. v. Haldeman, 559 F.2d 31 (D.C. Cir. 1976) (upholding conviction of violation of 18 U.S.C.A. § 371). One commentator has explained further how the statute was applied in the Watergate context:

> In criminal law, a conspiracy is an agreement "between two or more persons" to follow a course of conduct that, if completed, would constitute a crime. The agreement doesn't have to be express; most conspiracies are proved through evidence of concerted action. But government officials are expected to act in concert. So proof that they were conspiring requires a comparison of their public conduct and statements with their conduct and statements behind the scenes. A pattern of double-dealing proves a criminal conspiracy. The concept of interfering with a lawful government function is best explained by reference to two well-known cases where courts found that executive branch officials had defrauded the United States by abusing their power for personal or political reasons. One is the Watergate case, where a federal district court held that Nixon's Chief of Staff, H.R. Haldeman, and his crew had interfered with the lawful government functions of the CIA and the FBI by causing the CIA to intervene in the FBI's Investigation into the burglary of Democratic Party headquarters. The other is United States v. North, where the court found that Reagan Administration National Security Adviser John Poindexter, Poindexter's aide Oliver North and others had interfered with Congress's lawful power to oversee foreign affairs by lying about secret arms deals during Congressional

hearings into the Iran/contra scandal. Elizabeth De La Vega, *The White House Criminal Conspiracy*, THE NATION (Nov. 14, 2005)

b. Making False Statements to Congress (18 U.S.C. § 1001)

Federal law proscribes the submission of false statements or evidence to Congress or congressional committees. It is a criminal offense to knowingly and willfully:

(1) falsif[y], conceal, or cover up by any trick, scheme, or device a material fact; (2) make any materially false, fictitious, or fraudulent statement or representation; or (3) make or use any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry. 18 U.S.C. § 1001(a). The penalty includes a fine, imprisonment for not more than five years, or both. *Id.*

With respect to the proceedings before Congress, this prohibition applies to administrative matters and to "any investigation or review, conducted pursuant to the authority of any committee, subcommittee, commission or office of the Congress, consistent with applicable rules of the House or Senate." *Ibid.* § 1001(c). The statute's parameters were extended to Congress only in 1996. False Statements Accountability Act of 1996, Pub. L. No. 104-292, § 2, 110 Stat. 3459 (1996); *see also* United States v. Oakar, 111 F.3d 146, 151 (1997).

There is no limitation on the definition of what constitutes an "investigation or review" by Congress. As such, the term could encompass any hearing, markup, deposition, interrogatory, informal request for information, or speech before Congress or one of its committees or subcommittees. For example, Article II of the Constitution directs the President "from time to time [to] give to the Congress Information of the State of the Union, and recommend to their Consideration such Measures as he shall judge necessary and expedient." U.S. CONST. art. II, § 3. To further this requirement, a House concurrent resolution is agreed to by both chambers directing both Houses of Congress to assemble in the Hall of the House on the date and time for the address. *See* H.R. Con. Res. 20, 109th Cong., 1st Sess. (2005). As a result, even the President's State of the Union address could be considered an "investigation or review" conducted pursuant to Congress's authority.

In addition, legal treatises have further explained the meaning of the term "fraudulent misrepresentation." The term "fraudulent misrepresentation" includes "half truths calculated to deceive; and a half truth may be more misleading than an outright lie. A representation literally true is actionable if used to create an impression substantially false, as where it is accompanied by conduct calculated to deceive or where it does not state matters which materially qualify that statement." CORPUS JURIS SECUNDUM § 24. Francis T. Mandanici, "Bush's Uranium Lies: The Case for a Special Prosecutor That Could Lead to Impeachment," (June 29, 2005).

c. War Powers Resolution (Public Law 93-148)

It is unconstitutional and illegal for the President to engage the U.S. Armed Forces without timely congressional authorization. As a constitutional matter, the War Powers Clause, contained in article I, section 8, of the Constitution, gives Congress the sole authority to declare war.

As a statutory matter, in 1973 Congress passed the War Powers Resolution (WPR), which governs what powers the President is provided in order to send armed forces into hostilities absent a congressional declaration of war. War Powers Resolution, Pub. L. No. 93-148 (1973). The WPR requires the President to consult with Congress "in every possible instance" before sending troops into hostilities and to submit reports to Congress whenever forces are introduced. *Ibid.* Under the WPR, within sixty days after an initial report to Congress is submitted or should have been submitted, the President must terminate any use of armed forces unless Congress (1) declares war or authorizes the use of force, (2) extends the sixty-day period, or (3) cannot meet due to an attack on the United States. The D.C. Circuit Court of Appeals has interpreted this to mean that if the President engages U.S. armed forces, he has sixty days in which to obtain congressional authorization for the use of force or to cease such military activity. *See* Campbell v. Clinton, 203 F.3d 19, 20 (D.C. Cir. 2000).

d. Misuse of Government Funds (31 U.S.C. § 1301)

Federal law makes it illegal to use government funds appropriated to the government for any purpose other than those specifically permitted by the appropriations. It specifically states that "appropriations shall be applied only to the objects for which the appropriations were made except as otherwise provided by law." 31 U.S.C. § 1301. The illegal use of funds would cause an automatic diminution in funds available to the guilty agency. *Id*

To determine whether a government activity is legal, it is important to understand whether the agency or office that engaged in the activity was permitted to expend funds for that specific purpose. *See* U.S. GENERAL ACCOUNTING OFFICE, PRINCIPLES OF FEDERAL APPROPRIATIONS LAW 4-9 (3d ed. 2004). As a general rule, of course, none of the functions of government offices include the dissemination of false information, the dissemination of information for political ends, or retribution against political opponents. For example, the Constitution provides that the President shall be commander-in-chief of the Armed Forces, have the authority to grant pardons, have the power to sign treaties, and nominate civil officers and ambassadors and judges. U.S. CONST. art. II, § 2. Congress has provided funds to the President to hire staff and carry out his responsibilities; none of these appropriated funds is conditioned upon the President misleading the public or manipulating government agencies. *See* Pub. L. No. 108-7, Division J, title III (appropriations for fiscal year 2003 enacted in early 2003). The Constitution directs that the vice president will vote as a

tie-breaker in instances in which the Senate has a tie vote. U.S. CONST. art I, § 3. In addition, the vice president becomes the President when the President either is removed or otherwise unable to perform his duties. *Ibid.* amend. XXV.

Thus, the use of government funds for anything other than these enumerated purposes would violate the law. Using appropriated funds to criticize other officials or private citizens or to disseminate information for political purposes would be illegal.

2. Improper Detention, Torture, and Other Inhumane Treatment

Pursuant to federal law and numerous international treaties and conventions, the United States has the authority to prohibit and punish acts of torture and other inhumane treatment. The Justice Department has the authority to prosecute military contractors and other officials applying torture techniques in numerous ways: First, under the Military Extraterritorial Jurisdiction Act, which provides for the prosecution of anyone accompanying the military overseas, including military contractors. 18 U.S.C. §§ 3261-67 (2005). It was extended in 2004 to include contractors of other agencies, such as the CIA. Pub. L. No. 108-375, Div. A, Title X, § 1088, 118 Stat. 2066 (2004). Moreover, the Justice Department does have the authority to charge members of the military for their criminal acts over seas if either a) they are no long in the military, or b) committed the acts with non-military accomplices. Specifically, it allows the Justice Department to prosecute those acts over seas that would be felonies, crimes punishable by at least 6 months in prison, if committed on American soil. 18 U.S.C. §§ 3261-67 (2005).

a. Anti-Torture Statute (18 U.S.C. §§ 2340-40A)

Federal law prohibits torture, which is defined as: "an act committed by a person acting under the color of law specifically intended to inflict severe physical or mental pain or suffering . . . upon another person within his custody or physical control." 18 U.S.C. § 2340(1). This statute's application does not rely on the location of the abuse, the nationality of the victim, nor the combat or civilian status of the person in custody; all U.S. citizens are subject to the jurisdiction of this statute if they abuse those lawfully in their custody. AMNESTY INTERNATIONAL, DENOUNCE TORTURE (Nov. 2001), *available at* www.amnestyusa.org/stoptorture/law.html; Human Rights First, U.S. Law For Prosecuting Torture and Other Serious Abuses Committed by Civilians Abroad, *available at* www.humanrightsfirst.org/us_law/detainees/us_toture_laws.htm. This statute can also be used to prosecute foreign nationals who are apprehended on U.S. soil.

In practice, "torture" has been defined broadly by our own government. The military's own manual lists techniques such as the abuse of stress positions and sleep deprivation as torture and prohibits their use. HUMAN RIGHTS WATCH, GETTING AWAY WITH TORTURE: COMMAND RESPONSIBILITY FOR THE U.S. ABUSE OF DETAINEES, Apr. 2005 at 34 (citing

Army *Field Manual 34-52*). Further, our State Department has categorized other nations as human rights violators for practicing these precise techniques, including food, sleep and sensory deprivation, isolation and stress positions. Country Reports, U.S. Department of State, *available at* http://www.state.gov/g/drl/hr/c1470.htm.

It is also important to note that we have prosecuted others for war crimes for the same behavior. After World War II, the United States prosecuted hundreds of Japanese military members for abuse such as stress positions, sleep and sensory deprivation, forced nudity, solitary confinement and failure to notify the Red Cross of detainees. Jess Bravin, *Will Old Rulings Play a Role in Terror Case?*, WSJ, Apr. 7, 2005 at B1.

Those who order torture, or in other ways conspire to commit torture, can be held criminally liable under this statute - the statute doesn't require a person to actually commit torture with his own hands. AMNESTY INTERNATIONAL, DENOUNCE TORTURE (Nov. 2001), *available at* www.amnestyusa.org/stoptorture/law.html. In addition to the traditional conspiracy and aiding and abetting charges, military personnel and officials can be held liable under the command responsibility doctrine. *See* HUMAN RIGHTS WATCH, GETTING AWAY WITH TORTURE: COMMAND RESPONSIBILITY FOR THE U.S. ABUSE OF DETAINEES (Apr. 2005), *available at* http://www.hrw.org/reports/2005/us0405/. Conspiring to violate this prohibition is explicitly recognized in the statute and is punishable up to life in prison if death results, and for twenty years in prison otherwise. 18 U.S.C. § 2340A(c).

Notably, the Administration itself has recognized that its officials could be prosecuted for their role in condoning torture under this statute in particular. In fact, the Bush Administration has taken great pains to craft a legal defense to a charge under this statute noting that someday officials in the Bush Administration may be prosecuted for their role in the abuse of detainees.

b. The War Crimes Act (18 U.S.C. § 2441)

The War Crimes Act of 1996 criminalizes actions that would be either "grave breaches"

- of the Geneva Conventions Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135, [hereinafter "GC III"]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287, [hereinafter "GC IV"], (*entered into force* Oct. 21, 1950). The U.S. and Iraq are both parties to the Conventions.

- or violations of Common Article 3 of the Geneva Conventions. 18 U.S.C. § 2441 As President Bush has admitted himself, Iraqi detainees held in Iraq are covered by the Geneva Conventions. However, he maintains that non-Iraqis

captured in Iraq are not. *See* Terry Frieden, *Justice Dept: Geneva Conventions Limited in Iraq*, CNN.COM, Oct. 26, 2004, *available at* http://www.cnn.com/2004/LAW/10/26/noniraqi.prisoners/.

Grave breaches are defined within the Conventions as "wilful killing, torture or inhuman treatment, including biological experiments, willfully causing great suffering or serious injury to body or health;" (GC III, art. 130; GC IV art. 147) and "wilfully depriving a protected person of the rights of fair and regular trial prescribed in the present Convention." GC IV, art. 147. *See also* GC III, art. 130 which requires that Prisoners of War also receive fair trials. urther, it is a grave breach to remove a detained from the country where he is located, except when his removal is necessary for his own safety. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1), June 8, 1977, art. 85, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I] ("4. In addition to the grave breaches defined in the preceding paragraphs and in the Conventions, the following shall be regarded as grave breaches of this Protocol, when committed willfully and in violation of the Conventions or the Protocol:
(a) the transfer by the occupying Power of parts of its own civilian population into the territory it occupies, or the deportation or transfer of all or parts of the population of the occupied territory within or outside this territory, in violation of Article 49 of the Fourth Convention").

Common Article 3 prohibits "[v]iolence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;...outrages upon personal dignity, in particular humiliating and degrading treatment." GC III, art. 3; GC IV, art. 3.

The Administration has admitted it is subject to prosecution under this statute. The Attorney General in fact cited his concern with prosecution under the War Crimes Act as a justification for declaring Afghan detainees devoid of protection under the Geneva Conventions. Memorandum from White House Counsel Alberto R. Gonzales to President George W. Bush (Jan 25, 2002), *available at* http://www.humanrightsfirst.com/us_law/etn/gonzales/memos_dir/memo_20020125_Gonz_Bush.pdf.

Because this provision can only be used to prosecute abuse of those protected by the Conventions, withholding those protections would allow the government to use techniques barred by international law without fear of prosecution in American courts.

It is important to note that despite the focus in the media concerning what exactly constitutes "torture," "torture" isn't necessary to a conviction under this statute. It is just as much a war crime to:

1. treat a detainee "inhumanly"
2. cause "great suffering" or "serious injury"
3. denying detainees the right to a fair trial
4. practice "cruel treatment"
5. commit "outrages upon personal dignity, in particular humiliating and degrading treatment" GC III, art. 130; GC IV, art. 147; Additional Protocol 1, arts. 11, 85. *See* International Committee of the Red Cross, *How 'Grave Breaches' are Defined in the Geneva Conventions and Additional Protocols*, June 6, 2004, *available at* www.icrc.org.

c. The Geneva Conventions and Hague Convention: International Laws Governing the Treatment of Detainees

The United States, along with 191 other countries, is a party to the Geneva Conventions. The United States ratified the Conventions on February 8, 2005. The Geneva Conventions provide basic human rights to everyone in Iraq. Whether a combatant covered by the third Geneva Convention as a prisoner of war, or as a protected person (civilian) under the fourth Geneva Convention, detainees must be treated humanely. GC III, art. 13; GC IV, art. 27. Detainees are protected against "violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;...outrages upon personal dignity, in particular, humiliating and degrading treatment..." (GC III, art. 3; GC IV, art. 3.) and "wilfully depriving a protected person of the rights of fair and regular trial prescribed in the present Convention." GC IV, art. 147. *See also* GC III, art. 130, which requires that prisoners of war also receive fair trials. Additional protocols accepted by the United States clarify that no matter a person's status, they are to be protected against the above mentioned abuses. Additional Protocol I, art. 75.

Violation of the above provisions are considered "grave breaches" and obligate our government to investigate and punish those responsible. The Conventions make clear that it is up to participating countries to enforce its provisions, as it is the only way that those protections will be observed. JENNIFER ELSEA, U.S. TREATMENT OF PRISONERS IN IRAQ: SELECTED LEGAL ISSUES, CONG. RESEARCH SERV. 9-10 (May 24, 2004)

Member nations are required to provide the framework for such enforcement and then to use that framework once violations occur.

The Geneva Conventions afford many other protections that the U.S. is obligated to enforce, even if not through criminal prosecution. Those include:

- Holding civilians only as long as they are a demonstrable security risk, and then reviewing their detention at least every six months in an independent tribunal; GC IV, art. 41- 42.

- Allowing the International Committee of the Red Cross access to detainees/internees; GC IV, art. 143.

- Preventing the use of weapons that cause the "superfluous injury or unnecessary suffering" of combatants. GC Protocol I, art. 35(2). Similarly, civilians "shall enjoy general protection against dangers arising from military operations." GC Protocol I, art. 51.

Similarly, the Hague Conventions regulate the laws of war. An Annex to the Hague Conventions, entitled Respecting the Laws and Customs of War on Land, prohibits the use of weapons or other devices that cause unnecessary suffering. Convention on the Laws and Customs of War on Land (Hague IV Annex); October 18, 1907 (it is forbidden "to employ arms, projectiles, or material calculated to cause unnecessary suffering.).

d. United Nations Convention Against Torture, and Cruel, Inhuman and Degrading Treatment: International Laws Governing the Treatment of Detainees

The United States is also a party to the UN's Convention Against Torture and Cruel, Inhuman and Degrading Treatment, which prohibits the use of torture, defined as "any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person." Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Dec. 10, 1984, art.1, 1465 U.N.T.S. 85 (entered into force June 26, 1987) [hereinafter "CAT"]. The United States ratified the CAT on October 21, 1994.

Most notably, it also bans the use of cruel, inhuman and degrading treatment of those in U.S. custody, regardless of the nationality of the detainee or his combatant status. Although those terms are not defined, they have been limited in scope to those practices that are banned by the Fifth, Eighth and Fourteenth Amendments, which the Senate generally noted reflect the international case law interpreting at least the terms cruel and inhuman. When the Senate ratified this treaty it clarified "That the United States considers itself bound by the obligation under article 16 to prevent `cruel, inhuman or degrading treatment or punishment', only insofar as the term `cruel, inhuman or degrading treatment or punishment' means the cruel, unusual and inhumane treatment or punishment prohibited by the Fifth, Eighth, and/or Fourteenth Amendments to the Constitution of the United States." Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Aug. 30, 1990, S. Doc. No. 101-30, at 25-26. U.S. courts have stated that, "Generally, cruel, inhuman, or degrading treatment includes acts which inflict mental or physical suffering, anguish, humiliation, fear and debasement, which do not rise to the level of 'torture.'" Mehinovic v. Vuckovic, 198 F. Supp. 2d 1322, 1348 (N.D. Ga. 2002); Tachiona v. Mugabe, 234 F. Supp. 2d 401 (S.D.N.Y. 2002); Jama v. INS, 22 F. Supp. 2d 353 (D. N.J. 1998)

As Amnesty International explains, there is no distinct line between torture and CID, although the latter has been defined broadly to make sure nothing abhorrent can slip through a "loophole" in the definition. AMNESTY INTERNATIONAL, TORTURE AND THE LAW (November 2001) *at* www.amnestyusa.org/stoptorture/law.html. Behavior of this nature is prohibited by the Geneva Conventions and the Convention Against Torture.

However, Human Rights First has noted that other nations that have been subjected to terrorism for decades have refrained from using CID techniques. HUMAN RIGHTS FIRST, U.S. LAWS PROHIBITS TORTURE AND OTHER CRUEL, INHUMAN OR DEGRADING TREATMENT OR PUNISHMENT, *at* www.humanrightsfirst.org.

Israel and the United Kingdom, for example, have been fighting terrorism for years, yet their courts have upheld bans on CID treatment. *Ibid.* Noted legal expert and Professor Mary Ellen O'Connell reviewed the history of CID techniques and noted that "military and U.S. law enforcement officers know how to interrogate without using coercive or cruel techniques - as do the military and police of our peer nations. They have done so successfully for decades." Mary Ellen O'Connell, *Affirming the Ban on Coercive Interrogation*, 66 OHIO ST. L. J. ___ (2005) (forthcoming article on file with the House Judiciary Committee Democratic staff).

Our own courts interpreting these phrases will look at a totality of the circumstances to see if treatment rises to the level of a CID violation. Jama v. INS, 22 F. Supp. 2d 353 (D. N.J. 1998). For example, a federal court found cruel and inhuman treatment in a New Jersey prison used to hold illegal immigrants. Jama v. INS, 22 F. Supp. 2d 353 (D. N.J. 1998).

The court found the following treatment violated the ban on CID: sleep deprivation; forced nakedness; ethnic and sexual taunts; sexual touch less than and including sexual assault; deprivation of clothing; deprivation of fresh food; shackling of detainees to their beds; months of solitary confinement; and the trading of sexual favors from female detainees in exchange for the ability to contact their lawyers. *Ibid.* at 358-59.

This is consistent with international tribunals and other courts that have interpreted the ban on CID treatment. They have found that acts, which may not be illegal alone, when applied in concert can rise to the level of CID, including hooding, sleep deprivation, loud music, and long durations in stress positions. *Ibid.*

Again, the onus is on the member countries to enact whatever framework is necessary to deter and punish not only those who commit these acts, but those who are "complicit" in their execution. CAT, art. 4 ("Each State Party shall ensure that all acts of torture are offences under its criminal law. The same shall apply to an attempt to commit torture and to an act by any person which constitutes complicity or participation in torture."). This includes instituting "prompt and impartial

investigation, wherever there is reasonable ground to believe that an act of torture has been committed." *Ibid.* at art. 12.

Columnist Bob Herbert further noted:

> The Universal Declaration of Human Rights, adopted in 1948, states simply that "No one shall be subject to torture or cruel, inhuman or degrading treatment or punishment." The International Covenant on Civil and Political Rights, to which the U.S. is a signatory, states the same. The binding Convention Against Torture, negotiated by the Reagan administration and ratified by the Senate, prohibits cruel, inhuman and degrading treatment. . . . But since last year's [defense] bill, a strange legal determination was made that the prohibition in the Convention Against Torture against cruel, inhuman, or degrading treatment does not legally apply to foreigners held outside the U.S. They can, apparently, be treated inhumanely. This is the [Bush] administration's position, even though Judge Abe Sofaer, who negotiated the Convention Against Torture for President Reagan, said in a recent letter that the Reagan administration never intended the prohibition against cruel, inhuman or degrading treatment to apply only on U.S. soil. Bob Herbert, *Who Isn't Against Torture?*, N.Y. TIMES, Oct. 10, 2005, at A19.

e. Command Responsibility

The United States has long recognized the legal principle of command responsibility - that military officials can be held criminally responsible for acts of their subordinates if they knew - or should have known - of the transgressions and failed to stop them or even punish them after the fact. See HUMAN RIGHTS WATCH, GETTING AWAY WITH TORTURE: COMMAND RESPONSIBILITY FOR THE U.S. ABUSE OF DETAINEES, Apr. 2005.

In re Yamashita, 327 U.S. 1 (1946), the preeminent case on command responsibility, held that a commander could be held criminally responsibility for the actions of his subordinates. General Tomoyuki Yamashita, the military governor of the Philippines and commander of Japanese forces, argued that he could not be prosecuted for the war crimes committed by his soldiers during World War II. *Ibid.* However, the Supreme Court stated that the laws of war would be eviscerated if commanders could turn a blind eye to the criminal acts of their subordinates:

> Its purpose to protect civilian populations and prisoners of war from brutality would largely be defeated if the commander of an invading army could with impunity neglect to take reasonable measures for their protection. Hence the law of war presupposes that its violation is to be avoided through the control of the operations of

war by commanders who are to some extent responsible for their subordinates. *Ibid.* at 15.

Deciding that Yamashita would stand trial before military commissions for the atrocities committed by his soldiers, the court held that a commander has "an affirmative duty to take such measures as were within his power and appropriate in the circumstances to protect prisoners of war and the civilian population." *Ibid.* at 16. Yamashita was eventually found guilty of war crimes for failing to control his troops and executed. HUMAN RIGHTS WATCH, GETTING AWAY WITH TORTURE: COMMAND RESPONSIBILITY FOR THE U.S. ABUSE OF DETAINEES, Apr. 2005, Annex - A Note on Command Responsibility.

U.S. and international law has since developed a three prong test to impose command responsibility for military commanders and civilian officials with constructive control over military forces: (1) a superior-subordinate relationship must exist, (2) the superior must have knowledge or reason to know that a crime was about to be committed or had been committed, and (3) the superior failed to prevent the crime or punish it after the fact. *Ibid.* This doctrine is reflected in the current Army Field Manual, (U.S. Army Field Manual 27-10, The Law of Land Warfare (July 18, 1956), § 501.) guidelines for U.S. instituted military tribunals, (Department of Defense, Military Commission Instruction No. 2, Crimes and Elements for Trials by Military commission, Apr. 30, 2003, *available at* www.defenselink.mil.) individual recovery under the Alien Tort Claim Act (Kadic v. Karadzic, 70 F.3d 232 (2nd Cir. 1995); Xuncax v. Gramajo, 886 F.Supp. 162 (D.Mass.1995) and the Torture Victim Protection Act, (Ford v. Garcia, 289 F3d 1283, (11th Cir. 2002) (defining the three elements of command responsibility in an action under the Torture Victim Protection Act); Xuncax v. Gramajo, 886 F.Supp. 162 (D.Mass.1995) and international law. Study on Customary International Law, International Committee of the Red Cross, July 21, 2005, *available at* www.icrc.org. As the Ninth Circuit stated, "The principle of 'command responsibility' that holds a superior responsible for the actions of subordinates appears to be well accepted in U.S. and international law in connection with acts committed in wartime." Hilao v. Estate of Ferdinand Marcos, 103 F.3d 767 (9th Cir. 1996).

First, there must be a superior-subordinate relationship. Courts will find such a relationship where it is explicit, such as in the military command structure, but also where actual or effective control exists. Ford, 289 F.3d at 1290-91. It therefore can be extended to civilian and political superiors. Major Michael L. Smidt, *Yamashita Medina and Beyond: Command Responsibility in Contemporary Military Operations,* 164 MIL. L. REV. 155 (2000); HUMAN RIGHTS WATCH, GETTING AWAY WITH TORTURE: COMMAND RESPONSIBILITY FOR THE U.S. ABUSE OF DETAINEES, Apr. 2005, Annex - A Note on Command Responsibility.

Second, the superior must know, or have reason to know, that a crime was about to be committed, or had been committed. One military commentator has

explained that the "should have known" standard "is primarily linked to time. Where reports are received over time or where large numbers of crimes are committed by large numbers of subordinates, creating a basis of constructive notice, it is reasonable to say that the commander should have known." *Ibid.* at 199.

Finally, the superior must have either failed to prevent the violation he foresaw or failed punish it after it occurred. It is customary international law and now standard in U.S. courts that a superior has a duty to take all measures that are "necessary and reasonable" to prevent a crime by his subordinates. Ford, 289 F.3d at 1292-93. In other words, "[I]f the commander gains actual knowledge and does nothing, then he may become a principal in the eyes of the law in that by his inaction he manifests an aiding and encouraging support to his troops, thereby indicating that he joins in their activity and wishes the end product to come about." Major Michael L. Smidt, *Yamashita Medina and Beyond: Command Responsibility in Contemporary Military Operations*, 164 MIL. L. REV. 155, 198 (2000) (*citing* Kenneth A. Howard, *Command Responsibility for War Crimes*, 21 J. PUB. L. 7, 16 (1972). Some international courts have held that superiors "are even responsible for failure to prevent if they fail to take into account factors such as the age, training or similar elements that point to obvious conclusions regarding the likelihood that such crimes would be committed" (Ilias Bantekas, *The Contemporary Law of Superior Responsibility*, 93 AM. J. INT'L. L. 573, 590 (1999).)

This third prong may also be met when a superior to fails to investigate and punish a crime once it has occurred. Ford, 289 F.3d at 1292-93.

f. Material Witness (18 U.S.C. § 3144)

Federal law governs how individuals with information about a crime may be detained. Section 3144 of title 18, United States Code, provides that if the government was not certain that a subpoena would compel a witness to appear in court, then the court could issue a warrant for the person's detention as a material witness. 18 U.S.C. § 3144. The individual would have to be provided with access to counsel during detention. The person may not be held at all, however, if their testimony could be secured by a deposition. *Ibid.* Finally, the individual must be released when justice would no longer be served by the detention. *Ibid.*

3. Retaliating against Witnesses and Other Individuals

a. Obstructing Congress (18 U.S.C. § 1505)

It is a federal criminal offense to impede any due exercise of congressional authority. More specifically, section 1505 of title 18 makes it illegal to:

corruptly, or by threats or force, or by any threatening letter or communication influences, obstructs, or impedes or endeavors to influence, obstruct, or impede . . .

the due and proper exercise of the power of inquiry under which any inquiry or investigation is being had by either House, or any committee of either House or any joint committee of the Congress. 18 U.S.C. § 1505. The penalty for violations of this prohibition includes a fine, imprisonment for not more than five years, or both. *Ibid.*

In general, the statute prohibits persons from "corruptly" influencing or impeding the exercise of congressional power. This has been construed to apply to situations when the defendant causes another to violate his or her legal duty to Congress, such as by coercing or threatening a witness before Congress to testify falsely or inaccurately. United States v. Poindexter, 951 F.2d 369, 385 (D.C. Cir. 1991). It is not required that the defendant have gained anything from his or her conduct in order for that conduct to be corrupt within the meaning of the statute. *See ibid.* at 386.

Finally, it is important to recognize that a congressional inquiry does need not be formally authorized for the section 1505 prohibition to apply. Instead the courts have found:

> the question of whether a given congressional investigation is a 'due and property exercise of the power of inquiry' for purposes of § 1505 cannot be answered by a myopic focus on formality. Rather, it is properly answered by a careful examination of all the surrounding circumstances. If it is apparent that the investigation is a legitimate exercise of investigative authority by a congressional committee within the committee's purview, it should be protected by § 1505. . . . To give § 1505 the protective force it was intended, corrupt endeavors to influence congressional investigations must be proscribed even when they occur prior to formal committee authorization. United States v. Mitchell, 877 F.2d 294, 300 (4th Cir. 1989).

Thus, any exercise of a committee or Congress' power, formal or informal, is protected from corruptive influence or obstruction. It would be unlawful, therefore, for any person in an official or unofficial capacity to coerce another individual to provide false statements or testimony to Congress or to force such individual to respond inaccurately to any congressional inquiry. Such inquiry could be initiated pursuant to formal Committee action or merely as part of an informal investigation.

b. Whistleblower Protection (5 U.S.C. § 2302)

In 1989, Congress passed the Whistleblower Protection Act to ensure that those who came forward to expose lawlessness and waste in the federal government would not be discouraged by fear of reprisal. 5 U.S.C. § 2302.

5 U.S.C.A. § 2302 delineates different "prohibited personnel practices" and applies to almost every government agency employee. Excepted positions include those within the FBI, the CIA, the Defense Intelligence Agency, the National Security Agency and military employees of the Department of Defense. *Ibid.* at (a)(2)(B)-(C); Homeland and National Security Whistleblower Protections: The Unfinished Agenda, Project on Government Oversight, Apr. 28, 2005 at 5, 8 [hereinafter POGO Report]. Other non-covered agencies include the Government Accountability Office, Defense Mapping Agency, Airport Baggage Screeners and government contractors.

One of those prohibited practices is adverse employment actions for whistleblowing activities. For positions besides those listed above, the government is barred from taking, or failing to take, a personnel action in retaliation for the employee's:

Disclosure of information...which the employee or applicant reasonably believes evidences—

(i) a violation of any law, rule or regulation, or

(ii) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to pubic health or safety· 5 U.S.C.§ 2303(a). However, the employee's disclosure must be lawful itself for the employee to receive the statutory protection.

The head of the applicable agencies are responsible for ensuring these prohibited practices do not take place. *Ibid.* at (c). However, if they do, the employee may seek redress from the Office of Special Counsel, the Merit Systems Protection Board, and the federal court system. POGO Report, at 8.

c. The Lloyd-LaFollette Act (5 U.S.C. § 7211)

Also known as the "anti-gag rule," this statute passed in response to the Taft and Theodore Roosevelt Administrations' attempt to silence their employees. It ensures that agency employees can provide Congress with the information necessary to do its job. Memorandum from Jack Maskell, Cong. Research Serv., to the Honorable Charles Rangel at 4 (Apr. 26, 2004) [hereinafter Maskell Memo], *available at* http://www.pogo.org/m/gp/wbr2005/AppendixD.pdf. It states that:

> The Right of employees, individually or collectively, to petition Congress or a Member of Congress, or to furnish information to either House of Congress or to a committee or Member thereof, may not be interfered with or denied. 5 U.S.C. § 7211.

Far broader than the Whistleblower Protection Act, this statute applies to everyone in the government's employ, even those in the intelligence field that are

not protected under that statute. Moreover, it does not limit the sort of information that is protected. It reflects what the Supreme Court has found to be the fundamental right and necessity of Congress receiving information: "a legislative body cannot legislate wisely or effectively in the absence of information regarding conditions which the legislation is intended to affect or change." Maskell memo *supra* at 3. In fact, this right is so paramount that the Court has presumptively construed every statute in the U.S. banning information disclosure to not apply to Congress unless it very specifically states so. *Ibid.*

To give teeth to the Lloyd-LaFollette Act, Congress has repeatedly passed a spending restriction in the annual Treasury Appropriations bill to prevent paying the salary of anyone who interferes with an employee's effort to provide information to the Congress. The requirement is clear: federal money shall not be spent to help suppress the first amendment rights of federal employees:

> No part of any appropriation contained in this or any other Act shall be available for the payment of the salary of any officer or employee of the Federal Government, who--
>
> (1) prohibits or prevents, or attempts or threatens to prohibit or prevent, any other officer or employee of the Federal Government from having any direct oral or written communication or contact with any Member, committee, or subcommittee of the Congress in connection with any matter pertaining to the employment of such other officer or employee or pertaining to the department or agency of such other officer or employee in any way, irrespective of whether such communication or contact is at the initiative of such other officer or employee or in response to the request or inquiry of such Member, committee, or subcommittee; or
>
> (2) removes, suspends from duty without pay, demotes, reduces in rank, seniority, status, pay, or performance of efficiency rating, denies promotion to, relocates, reassigns, transfers, disciplines, or discriminates in regard to any employment right, entitlement, or benefit, or any term or condition of employment of, any other officer or employee of the Federal Government, or attempts or threatens to commit any of the foregoing actions with respect to such other officer or employee, by reason of any communication or contact of such other officer or employee with any Member, committee, or subcommittee of the Congress as described in paragraph (1). *See e.g.* H.R. 3058, 109th Cong. § 918 (2005) (as engrossed by the House); S. 1446, 109th Cong. (2005); *see also*, for example, Consolidated Appropriations Act, 2005, Pub. L. No. 108-447, § 618 of Division H, 118 Stat. 2809 (2004); Consolidated Appropriations Act, 2004, Pub. L. No. 108-99, § 618 of Division F, 117 Stat. 1176 (2003); Consolidated Appropriations

Resolution, 2003, Pub. L. No. 108-7, §§ 617, 620, 117 Stat. 11 (2003); Treasury and General Government Appropriations Act of 2002, Pub. L. No. 107-67, §§ 617, 620, 115 Stat. 514 (2001).

d. Retaliating against Witnesses (18 U.S.C. § 1513)

The government may not retaliate against individuals who provide truthful information to law enforcement officials. Section 1513(e) of title 18 prohibits anyone from "knowingly, with the intent to retaliate, takes any action harmful to any person, including interference with the lawful employment or livelihood of any person, for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any Federal offense . . . ." 18 U.S.C. § 1513(e).

The term "law enforcement officer" is defined as "an officer or employee of the Federal Government . . . or serving the Federal Government as an adviser or consultant (A) authorized under law to engage in or supervise the prevention, detection, investigation, or prosecution of an offense; or (B) serving as a probation or pretrial services officer under this title." 18 U.S.C. § 1515(a)(4). The penalty for witness retaliation consists of a fine, imprisonment for not more than 10 years, or both. 18 U.S.C. § 1513(e).

Because of the definition of "law enforcement officer," this statute would apply to retaliating against any federal employee with investigative authority. For instance, a "law enforcement officer" would include any Justice Department employee (including attorneys, FBI agents, DEA agents, and ATFE agents) as well as inspectors general. This is because each inspector general must "provide policy direction for and to conduct, supervise, and coordinate audits and investigations relating to the programs and operations of [the relevant office]." 5 U.S.C. app. 3, § 4 (emphasis added). Any person who informed such officials of violations of federal law would be protected from any form of retaliation, such as firing, demotion, or rescission of security clearance or other tools necessary for job performance.

A violation of section 1513 is a predicate offense under RICO. 18 U.S.C. § 1961. It thus is unlawful to acquire and invest income or to acquire any interest in any enterprise through a pattern of section 1513 violations. *Ibid.* § 1962. Penalties for violating RICO include a fine, imprisonment for not more than twenty years, or both, as well as forfeiture of any proceeds from the illegal activity. *Ibid.* § 1963.

Finally, it is a separate criminal offense to conspire to commit the crime of witness retaliation. *Ibid.* § 1513. The penalty for conspiring to commit such an offense is the same as for the crime that was the object of the conspiracy.

4. Leaking and other Misuse of Intelligence and other Government Information

Numerous federal laws and regulations make it a crime to disclose national security or intelligence information without proper authorization.

a. Revealing Classified Information in Contravention of Federal Regulations (Executive Order 12958/ Classified Information Nondisclosure Agreement

First, there are administrative sanctions for misuse of classified information. Presidential Executive Order 12958 prescribes a uniform system for classifying, declassifying, and protecting information related to the national defense. Exec. Order No. 12948, 32 C.F.R. § 2001.10 *et seq.* (2005). It requires each agency head to implement controls over the distribution of classified information. *Ibid.* Section 5.5 provides that, if the Director of the Information Security Oversight Office finds a violation of the Order has taken place, the Director must report to the appropriate agency head so correction action may occur. *Ibid.* Further, sanctions for such violations include: "reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation." *Ibid.*

The Order further requires that the supervisors of those who divulge classified information take remedial action against such officials. Such action can include the removal of security clearance and other measures to prevent further disclosure.

In effect, any supervisor of an individual with access to classified information must sanction such individual if he or she illegally discloses the information. For instance, the President would be responsible for ensuring that White House officials and staff having access to classified information complied with the Executive Order and would have to punish any such individual who violated the Order.

Also, prior to obtaining access to classified information, government officials must sign a Classified Information Nondisclosure Agreement, known as a Standard Form 312 or SF-312. The Agreement states that breaches (i.e., disclosure of classified information) could result in the termination of security clearances and removal from employment. The Agreement, signed by White House officials such as Mr. Rove, states: "I will never divulge classified information to anyone" who is not authorized to receive it. INFORMATION SECURITY OVERSIGHT OFFICE, CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (STANDARD FORM 312): BRIEFING BOOKLET 73 (emphasis added). *See also* The Honorable Henry A. Waxman, Ranking Member, U.S. House Comm. on Gov't Reform, Fact Sheet: Karl Rove's Nondisclosure Agreement 1-2 (July 15, 2005).

It also is important to note that even confirming the accuracy of classified information in a public source is a violation of the agreement. INFORMATION SECURITY OVERSIGHT OFFICE, CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (STANDARD FORM 312): BRIEFING BOOKLET 73 (emphasis added). *See also* The Honorable Henry A. Waxman, Ranking Member, U.S. House Comm. on Gov't Reform, Fact Sheet: Karl Rove's Nondisclosure Agreement 1-2 (July 15, 2005).

The agreement specifically states:

However, before disseminating the [classified] information elsewhere or confirming the accuracy of what appears in the public source, the signer of the SF 312 must confirm through an authorized official that the information has, in fact, been declassified. If it has not, further dissemination of the information or confirmation of its accuracy is also an authorized disclosure. INFORMATION SECURITY OVERSIGHT OFFICE, CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (STANDARD FORM 312): BRIEFING BOOKLET 73.

In short, if a White House official signs the agreement yet proceeds to disclose or confirm classified information, the President would be required to terminate that individual's security clearance and remove him or her from their position.

b. Statutory Prohibitions on Leaking Information

Numerous federal statutes make it a criminal offense to convey anything of value that belongs to the United States. Section 641 of title 18 imposes criminal penalties on anyone who "embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys, or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof." 18 U.S.C. § 641. The penalty for a violation of this statute is a fine, imprisonment for not more than ten years, or both; however, if the value of the property is less than $1,000, then the prison term cannot exceed one year. *Ibid.*

This statute has been interpreted broadly, giving latitude to what constitutes a "thing of value." The Fourth Circuit Court of Appeals has held that the classification of information is, in and of itself, relevant to determining whether that information is a "thing of value" to the United States. United States v. Zettl, 889 F.2d 51, 54 (4th Cir. 1989). Similarly, the Sixth Circuit ruled that the term pertains to both tangible and intangible property. United States v. Jeter, 775 F.2d 670 (6th Cir. 1985). The Bush Justice Department has already determined that government information is a "thing of value." *See* John Dean, *It Doesn't Look Good for Karl Rove*, CNN.COM, July15, 2005, *available at* http://www.cnn.com/2005/LAW/07/15/dean.rove/. Jonathan Randel, a former Drug Enforcement Administration employee, leaked to the British media the fact that the name Lord Michael Ashcroft of Great Britain appeared in the DEA's money laundering files. Press Release, U.S. Attorneys' Office, Northern District of Georgia, Former DEA Worker Sentenced to Prison for Selling Information (Jan. 9, 2003), *available at* http://www.usdoj.gov/usao/gan/press/01-09-03_2.html. In 2002, the Justice Department obtained an indictment against Mr. Randel for violating section 641. Mr. Randel ultimately pled guilty and was sentenced to one year in prison and three years of probation. *Id.* While he was sentencing Mr. Randel, U.S. District Judge Richard Story stated, "Anything that would affect the security of officers and of the operations of the agency would be of tremendous concern, I think, to any law-abiding citizen in this country." John Dean, *supra*.

Because "thing of value" is a broad term, the prohibition in turn is broad. Information such as U.S. intelligence data or analyses could be considered "of value" and thus prohibited from disclosure, even such information is not classified. Even analyses of foreign military and defense capabilities would be protected as "of value" to the United States.

The *mens rea*, or intent, requirement under the statute also is interpreted broadly. The government need only establish that the defendant transmitted information without authority. *Jeter*, 775 F.2d at 681. It is irrelevant whether the defendant knew the information was "of value" to the United States. *See Ibid.*

Second, it is illegal for any person to willfully disclose information related to the national defense. Subsection 793(d) of title 18 applies to persons having lawful possession of vital information. Criminal liability assigns to anyone:

> who has lawful possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, [and] willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, or transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it." 18 U.S.C. § 793(d).

The penalty for violating this prohibition includes a fine, imprisonment for not more than ten years, or both. *Id.* § 793. The penalty for conspiring to commit such an offense, and engaging in any act in furtherance of such, is the same as for the underlying offense. *Id.* § 793(g).

This means that it is unlawful to divulge any information related to U.S. military bases, defense installations, war plans, intelligence capabilities, or intelligence information. As stated above this prohibition applies to officials and employees who have lawful access to the information in question.

Courts have construed this prohibition broadly. For instance, prohibited disclosures are not limited to foreign agents; it is illegal to disclose defense information to the media, as well. United States v. Morison, 844 F.2d 1057 (4th Cir. 1988). Further, it is not necessary for the information in question to be classified for it to be protected from disclosure. United States v. Harris, 40 C.M.R. 308 (1969).

Third, it is a highly serious offense to transmit any defense information to a foreign agent or foreign government, regardless of whether the foreign entity is friendly or an enemy. *See* United States v. Rosenberg, 195 F.2d 583 (2d Cir.1952). Subsection 794(a) of title 18 prohibits the transmission or delivery of any document or information related to national defense to any foreign government or foreign agent. 18 U.S.C. § 794(a). The penalty includes death (in cases involving death of an American agent or military systems) or imprisonment for any term of years. *Id.* The penalty for conspiring to commit such an offense, and engaging in any act in furtherance of such, is the same as for the underlying offense. *Id.* § 794(c).

Such conduct is illegal if the transmission is direct or indirect. *Ibid.* § 794(a). The disclosure must occur with the intent or reason to believe that it would be used to injure the United States or to the advantage of a foreign nation. *Ibid.*

In other words, government officials and private citizens are prohibited from leaking to foreign governments any information related to our national defense. This prohibition applies to information about U.S. intelligence capabilities, military plans, defense strategy, or knowledge of foreign military assets. Any person who released such information later obtained by a foreign government, whether through speeches or press releases or leaks to the news media, would be acting unlawfully.

Finally, it also can be a specific federal crime to disclose the name of a covert U.S. agent. Subsection 421(a) of title 50 makes it unlawful for someone, having or having had access to classified information that identifies a covert agent, to intentionally disclose such information to an unauthorized recipient knowing the disclosure identifies the agent and knowing that the government is taking affirmative measures to conceal the agent's relationship to the United States. 50 U.S.C. § 421(a). The penalty includes a fine, imprisonment for not more than ten years, or both. *Ibid.* Similarly, subsection 421(b) of title 50 makes it unlawful for someone who, as a result of having access to classified information, learns the identity of a covert agent and intentionally discloses any information disclosing that identity to any person not authorized to receive it. The defendant must know that the information disclosed identifies the agent and that the government is taking steps to conceal the identity. *Ibid.* § 421(b). The penalty includes a fine, imprisonment for not more than five years, or both. *Ibid.* As such, it is a crime to intentionally disclose the identity of a covert agent to someone who is not allowed to have the information. Our review indicates that no prosecutions have been brought under this section 421 of title 50.

5. Laws and Guidelines Prohibiting Conflicts of Interest

Existing law and rules of professional conduct govern when Department attorneys must recuse themselves from particular investigations. Federal law requires the Attorney General to promulgate rules mandating the disqualification of any officer or employee of the Justice Department "from participation in a particular

investigation or prosecution if such participation may result in a personal, financial, or political conflict of interest, or the appearance thereof." 28 U.S.C. § 528 (emphasis added). Pursuant to this requirement, the Department has promulgated regulations stating that:

> No employee shall participate in a criminal investigation or prosecution if he has a personal or political relationship with: (1) any person . . . substantially involved in the conduct that is the subject of the investigation or prosecution; or (2) any person . . . which he knows or has a specific and substantial interest that would be affected by the outcome of the investigation or prosecution. 28 C.F.R. § 45.2.

To reiterate the importance of preventing conflicts of interest, the Justice Department has further explicated the guidelines in its U.S. Attorneys' Manual. The Attorneys' Manual provides that:

When United States Attorneys, or their offices, become aware of an issue that could require a recusal in a criminal or civil matter or case as a result of a personal interest or professional relationship with parties involved in the matter, they must contact General Counsel's Office (GCO), EOUSA. The requirement of recusal does not arise in every instance, but only where a conflict of interest exists or there is an appearance of a conflict of interest or loss of impartiality. U.S. DEP'T OF JUSTICE, U.S. ATTORNEYS' MANUAL § 3-2.170.

Furthermore, rules of professional conduct bar lawyers from matters in which they have conflicts of interest. Because Department attorneys must follow the ethical rules of the bar in which they practice, 28 U.S.C. § 530B, officials at Main Justice are obligated to comply with the District of Columbia Bar's Rules of Professional Conduct. These Rules state that, without consent, a lawyer shall not represent a client if "the lawyer's professional judgment on behalf of the client will be or reasonably may be adversely affected by the lawyer's responsibilities to or interests in a third party or the lawyer's own financial, business, property, or personal interests." DISTRICT OF COLUMBIA BAR, RULES OF PROFESSIONAL CONDUCT 1.7(b)(4). The American Bar Association mimics this guideline in Rule 1.7 of its own Model Rules of Professional Conduct. *See* AMERICAN BAR ASSOCIATION, MODEL RULES OF PROFESSIONAL CONDUCT 1.7(a)(2).

6. Laws Governing Electronic Surveillance

The general rule regarding electronic surveillance is that it is illegal for any person to "engage in electronic surveillance under color of law except as authorized by statute." 50 U.S.C. § 1809.

There are two statutes that govern electronic surveillance: (1) Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act"), 18 U.S.C. §§

2510-2521.which governs wiretapping in criminal cases; and (2) the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. § 1801 *et seq.* which governs electronic surveillance of foreign powers or agents of foreign powers in national security investigations. These two statutes are the "exclusive means by which electronic surveillance ... and the interception of wire and oral communication may be conducted." 18 U.S.C. § 2511.

a. Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 et seq)

In discussing Presidential authority to conduct warrantless electronic surveillance to gather foreign intelligence, the Foreign Intelligence Surveillance Act (FISA) is the applicable statute. In fact, FISA applies to the "interception of international wire communications to or from any person (whether or not a U.S. person) within the United States without the consent of at least one party" (Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, Title I, 92 Stat. 1796 (Oct. 25, 1978) codified as amended. Under FISA, the government must seek an order from the FISA court (sometimes referred to as a FISA "warrant") before conducting electronic surveillance for foreign intelligence information. The application for the order must state that there is probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power. 50 U.S.C. § 1805. For example, if a U.S. citizen, who is suspected of terrorist activity, is talking on his telephone from his home in Virginia. The government must obtain a FISA warrant prior to monitoring his calls.

Exceptions to this warrant requirement exist when there is an emergency and during wartime. If the Attorney General certifies that there is an emergency need to conduct electronic surveillance, he may authorize the surveillance, but must apply for a FISA warrant as soon as practicable, and not more than 72 hours later. *Ibid.* § 1805(f). For example, if a U.S. citizen, who is suspected of terrorist activity, begins talking on his telephone, the government can begin monitoring his conversations without a warrant but must apply for the warrant within 72 hours.

Wartime also creates an exception to FISA's warrant requirement. FISA expressly governs wiretapping procedures "during time of war" and provides that "the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for a period not to exceed fifteen days following a declaration of war by the Congress." *Ibid.* § 1811.

If the electronic surveillance is directed solely at communications between or among foreign powers and there is "no substantial likelihood" that the surveillance will acquire the contents of any communication to which a U.S. person is a part, then the President may authorize surveillance without a FISA warrant for up to one year. *Ibid.* § 1802. A U.S. person is defined under FISA as a citizen, a lawful permanent

resident, a U.S. corporation, or an unincorporated association a substantial number of members of which are U.S. citizens.

FISA's most notable provisions in this particular context are provisions that make criminal any electronic surveillance not authorized by statute *(Ibid.* § 1809.) and provisions that expressly establish FISA and specified provisions of the federal criminal code as the "exclusive means by which electronic surveillance . . . may be conducted." 18 U.S.C. § 2511(2)(f).

b. National Security Act of 1947 (50 U.S.C. chapter 15)

The National Security Act of 1947, and amendments thereto, governs the nation's counterintelligence apparatus. 50 U.S.C. chapter 15. Briefings are limited to the Gang of Eight only when intelligence activities involve "covert action" or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent." 50 U.S.C. § 413b(e). Covert actions, pursuant to the statute, do not include "activities the primary purpose of which is to acquire intelligence." *Ibid.* § 413b(e)(1).

Unless a "covert action" is involved, the National Security Act requires that "the President shall ensure that the congress intelligence committees are kept fully and currently informed of the intelligence activities of the United States." *Ibid.* § 413(a)(1). The Act makes clear that the requirement to keep the committees informed may not be evaded on the grounds that "providing the information to the congressional intelligence committees would constitute the unauthorized disclosure of classified information." *Ibid.* § 413(e).

c. Communications Act of 1934 (47 U.S.C. § 222)

Section 222 of the Communications Act generally states that every telecommunications carrier has a duty to protect the confidentiality of the proprietary information of their customers. 47 U.S.C. § 222(a). Proprietary information is: (a) information that relates to the quantity, technical configuration, type, destination, location, an amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available by the customer solely by virtue of the carrier-customer relationship; and (b) information contained in the bills pertaining to telephone exchange service or telephone service received by a customer of a carrier. *Id.* § 222(h)(1)(A-B).A carrier may only use, disclose, or permit access to individually-identifiable customer information in its provision of the telecommunications service or services necessary to the provision of such service. *Ibid.* § 222(c)(1). The law provides that the carrier may disclose such information if it is required by law, if it has customer approval, or if it falls under one of the exceptions outlined in the chapter. *Ibid.* § 222.

The Communications Act provides several exceptions to the prohibition on disclosure of communications content. Specifically, the law provides that a carrier may disclose the content of communications in order to (1) provide or initiate services and collect or bill for services rendered; (2) to protect the rights or property of the carrier, or to protect users of those services from fraudulent, abusive, or unlawful use of, or subscription to, such services; (3) to provide telemarketing, referral, or administrative services to the customer; or (4) to provide call location information in the case of an emergency. *Ibid.* § 222(d).

Carriers in violation of the requirements provided in the Communications Act are subject to a variety of penalties under the Act. Specifically, the law provides for criminal penalties for any knowing and willful violation of any provision of the Act. 47 U.S.C. § 501. The resulting criminal penalty provided by the Act is a fine of up to $10,000, imprisonment for up to one year, or both; and in the case of a person previously convicted of violating the Act, a fine up to $10,000, imprisonment up to two years, or both. *Ibid.* In addition, the law also punishes the willful and knowing violations of Federal Communication Commission regulations that result from a violation of the Act. *Ibid.* § 502. This section provides that any person who willfully and knowingly violates any rule, regulation, restriction, or condition made or imposed by the Commission is, in addition to other penalties provided by law, subject to a maximum fine of $500 for each day on which a violation occurs. *Ibid.*

d. Stored Communications Act of 1986 (18 U.S.C. § 2702)

Under the Stored Communications Act of 1986, it is a federal criminal offense for a provider of electronic communications services or of remote computing services to disclose the contents of a communication that are in electronic storage. 18 U.S.C. § 2702(a). The penalty for violating this prohibition is a fine and up to ten years imprisonment for serious and repeat offenders. *Ibid.* § 2701. In addition, persons harmed by knowing or intentional violations of the law may bring civil actions in court for damages, attorney's fees, and equitable relief. *Ibid.* § 2707.

Exceptions to the prohibition on disclosure of communications content exist, such as for transmissions that are incident to the provision of communications service and pursuant to specific criminal statutes. *Ibid.* § 2702(b). There is also an exception wherein a provider may divulge a communication to a governmental entity if, in good faith, the provider believes that an emergency involving danger of death or serious physical injury to any person requires disclosure. *Ibid.* Furthermore, in analyzing another statute that permits voluntary disclosure of customer records, a court has held that there must be a good faith nexus between the alleged suspicious activity and the disclosure of the protected information for there to be statutory protection for the disclosure. Lopez v. First Union Nat'l Bank, 129 F.3d 1186 (11th Cir. 1997). Defendant evoked the safe harbor provision of the Annunzio-Wylie Anti-Money Laundering Act of 1992 (31 U.S.C. § 5318 (g)(3)).

There also are exceptions that allow for disclosure of customer records. 18 U.S.C. § 2702(c). These include: the consent of the subscriber, necessarily incident to the provision of service, to a government entity if the provider believes an emergency involving danger of death or serious injury requires disclosure. *Ibid.* Additional provisions of the Stored Communications Act require that the Attorney General submit to the Committee on the Judiciary in both the House and the Senate a report containing the number of accounts from which the Department of Justice has received voluntary disclosures under the emergency exception, and a summary for the basis of those disclosures in some instances on an annual basis. 18 U.S.C. § 2702(d).

e. Pen Registers or Trap and Trace Devices (18 U.S.C. § 3121)

Pen registers are surveillance devices that capture in real-time the phone numbers dialed on outgoing telephone calls; (18 U.S.C. § 3127(3)) trap and trace devices capture the numbers identifying incoming calls. 18 U.S.C. § 3127(4). These devices are not designed to reveal the content of communications, or even identify the parties to a communication or whether a call was connected at all. The law on pen registers and trap and trace devices expressly prohibits their installation and use without first obtaining a court order either under the criminal wiretap law (18 U.S.C. § 3123.) or under FISA. 18 U.S.C. § 3121. This prohibition does not apply to use by an electronic or wire service provider relating to the operation, maintenance and testing of a service or protection of the rights or property of the service provider, or to use where the consent of the user of the service has been obtained. *Ibid.* Furthermore, a government agency authorized to install and use a pen register or trap and trace device under the provisions of this statute, must use technology reasonably available to it that restricts the recording or decoding of electronic impulses utilized in the processing and transmitting of wire or electronic communications in a manner that does not include the contents of that communication. 18 U.S.C. § 3123.